GENERAL SERVICES ADMINISTRATION
Federal Acquisition Service
Assisted Acquisition Services Division
Southeast Sunbelt Region

Task Order ID: ID04180034 **Date: February 13, 2018** **Version 2.0, updated effective 15 September 2018** **Mod 001: remove FAR 52.217-9, incorporate FAR clause 52.217-8, Option to Extend Services and update paragraph 1.5** **Mod 002: Exercise 6 month POP Extension of Services Option IAW FAR 52.217-8, Option to Extend Services)**	**GSA Customer Account Manager:** Name: Yvonne Powell Address: 77 Forsyth Street SW Atlanta, GA 30303-3490 Phone: (404) 331-9615 E-mail: yvonne.powell@gsa.gov **GSA Senior Contracting Officer (SCO):** Name: Matthew Wright Address: 77 Forsyth Street SW Atlanta, GA 30303-3490 Phone: (404) 983-6850 E-mail: Matthew.Wright@gsa.gov
Client Organization: United States Transportation Command (USTRANSCOM), Joint Communications Support Element (JCSE), JCSE HSS/J8 MacDill AFB, FL	**Primary Contracting Officer's Representative (COR):** Yolanda Dean Functional Director, Contract Joint Communications Support Element (JCSE) MacDill AFB, FL Phone: (404) 983-6850 Email: Yolanda.r.dean.civ@mail.mil
Task Title: Joint Communications Support Element (JCSE) Enterprise Network Service Support (ENNS)	**Period of Performance:** Base Period 03/15/2018 – 09/14/2018 Option (Exercised) 09/15/2018 - 03/14 /2019

☒	Firm Fixed Price	☒	Severable
☐	Labor Hour	☐	Non-Severable
☐	Time and Material		
		☒	Fully Funded
☒	Performance-based	☐	Incrementally Funded

PERFORMANCE WORK STATEMENT (PWS)

Task Order ID0418034

Date: February 13, 2018

Joint Communications Support Element (JCSE) Enterprise Network Service Support

Part 1

General Information

1. **GENERAL:** This is a non-personal services contract to provide Enterprise Network Information Technology (IT) Services Support. The Government shall not exercise any supervision or control over the contract service providers performing the services herein. Such contract service providers shall be accountable solely to the Contractor who, in turn, is responsible to the Government.

    1.1. Description of Services/Introduction: The contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items and non-personal services necessary to perform Network operations Center Services Support as defined in this Performance Work Statement except for those items specified as government furnished property and services. The contractor shall perform to the standards in this contract.

    1.2. Background: The Joint Communications Support Element (JCSE) provides overall Information Technology (IT) services in support of Agencies, Services Components, Combatant Commands, and directed contingency missions worldwide. This support includes all tasks necessary to ensure an effective IT and Information Management structure that fosters timely deployment and optimal operation of all JCSE Information Systems and IT resources.

    1.3. Objectives: The objective of this contract is to obtain a broad range of high quality contractors to support the Joint Communications Support Element network support services, as described in PWS.

    1.4. Scope: Provides effective, efficient, secure, and reliable information network services in executing its global mission and in support of its customers. Staff will operate, secure, and manages JCSE's Tactical Global Enterprise Network (GEN) and assets to provide C4ISR service capability worldwide across the full spectrum of operations in support of combatant commands (CCMD), joint forces headquarters (JFHQ), and other organizations and agencies as directed.

    1.5. Period of Performance: The period of performance shall be as follows:
    Base period: March 15, 2018 through September 14, 2018
    Option Period (exercised): September 15, 2018 through March 14, 2019

    1.6. General Information

1.6.1. Quality Control: The Contractor shall ensure all work will be performed in accordance with the contract requirements, in compliance with the FAR clause 52.212-4, paragraph entitled "Inspection/Acceptance". The contractor shall maintain, and submit to the Government within 10 days after award, a complete Quality Control Plan (QCP) addressing the inspection system used to ensure the requirements of this contract are met. The QCP shall be submitted with the proposal for evaluation by the Government during evaluation of the technical proposal in response to the solicitation. The contracting officer shall notify the contractor of acceptance or any required modifications. Acceptance of the plan by the contracting officer is required prior to the start of performance. The QCP shall include the following minimum requirements:

- A description of the inspection system to cover all major services and deliverables. The description shall include specifics as to the areas to be inspected on both a scheduled and unscheduled basis, frequency of inspections, and the title of inspectors.
- A description of the methods to be used for identifying and preventing defects in the quality of service performed.
- A description of the records to be kept to document inspections and corrective or preventative actions taken.
- All records of inspections performed shall be retained and made available to the Government upon request throughout the contract performance period, and for the period after contract completion, until final settlement of any claims under this contract.

1.6.2. Quality Assurance: The government shall evaluate the contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan. This plan is primarily focused on what the Government must do to ensure that the contractor has performed in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable deficiency rate(s).

1.6.3. Recognized Holidays: The contractor is not required to perform services on the following holidays:

New Year's Day	Labor Day
Martin Luther King Jr.'s Birthday	Columbus Day
President's Day	Veteran's Day
Memorial Day	Thanksgiving Day
Independence Day	Christmas Day

1.6.4. Hours of Operation: Identified contractors will provide 24/7 shift support. The 24/7 shifts will consist of 0700-1900 and 1900-0700, not to exceed 80 hours a pay period. The remaining contractors will be on 24/7 phone call and are responsible for conducting business, between the hours of 0700 – 1700, Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. Exception: Mission essential surge personnel, capable of globally deploying within 72 hours of notification.

1.6.5. The Contractor must at all times, maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons. When hiring personnel, the Contractor shall keep in mind that the stability and continuity of the workforce are essential.

1.6.6. Dress Code

1.6.6.1. Business Casual – projects a professional, business-like image while enjoying the advantage of more casual and relaxed.

1.6.6.1.1. Business casual includes slacks or khakis, dress shirt or blouse, open collar or polo shirt, optional tie or seasonal sport coat, a dress or skirt at knee-level or below, a tailored blazer, knit shirt or sweater, and loafers or dress shoes that cover all or most of the foot.

1.6.7. Place of Performance: The work to be performed under this contract will be performed at JCSE compound, MacDill AFB, FL or designated temporary duty locations or deployable locations.

1.6.8. Type of Contract: The government will award a Firm Fixed Price (FFP) contract.

1.6.9. Security Requirements: Contractor personnel performing work under this contract must have a Secret or Top Secret clearance, as identified in the PWS at time of the proposal submission, and must maintain the level of security required for the life of the contract. The security requirements are in accordance with the submitted DD254.

1.6.9.1. Physical Security: The contractor shall be responsible for safeguarding all government equipment, information and property provided for contractor use. At the close of each work period, government facilities, equipment, and materials shall be secured.

1.6.9.2. Key Control: The Contractor shall establish and implement methods of making sure all keys/key cards issued to the Contractor by the Government are not lost or misplaced and are not used by unauthorized persons. NOTE: All references to keys include key cards. No keys issued to the Contractor by the Government shall be duplicated. The Contractor shall develop procedures covering key control that shall be included in the Quality Control Plan. Such procedures shall include turn-in of any issued keys by personnel who no longer require access to locked areas. The Contractor shall immediately report any occurrences of lost or duplicate keys/key cards to the Contracting Officer.

1.6.9.2.1. In the event keys, other than master keys, are lost or duplicated, the Contractor shall, upon direction of the Contracting Officer, re-key or replace the affected lock or locks; however, the Government, at its option, may replace the affected lock or locks or perform re-keying. When the replacement of locks or re-keying is performed by the Government, the total cost of re-keying or the replacement of the lock or locks shall be deducted from the monthly payment due the Contractor. In the event a master key is lost or duplicated, all locks and keys for that system shall be replaced by the Government and the total cost deducted from the monthly payment due the Contractor.

1.6.9.2.2. The Contractor shall prohibit the use of Government issued keys/key cards by any persons other than the Contractor's employees. The Contractor

shall prohibit the opening of locked areas by Contractor employees to permit entrance of persons other than Contractor employees engaged in the performance of assigned work in those areas, or personnel authorized entrance by the Contracting Officer.

1.6.9.3. Lock Combinations: The Contractor shall establish and implement methods of ensuring that all lock combinations are not revealed to unauthorized persons. The Contractor shall ensure that lock combinations are changed when personnel having access to the combinations no longer have a need to know such combinations. These procedures shall be included in the Contractor's Quality Control Plan.

1.6.10. Post Award Conference/Periodic Progress Meetings: The Contractor agrees to attend any post award conference convened by the contracting activity or contract administration office in accordance with Federal Acquisition Regulation Subpart 42.5. The contracting officer, Contracting Officers Representative (COR), and other Government personnel, as appropriate, may meet periodically with the contractor to review the contractor's performance. At these meetings the contracting officer will apprise the contractor of how the government views the contractor's performance and the contractor will apprise the Government of problems, if any, being experienced. Appropriate action shall be taken to resolve outstanding issues. These meetings shall be at no additional cost to the government.

1.6.11. Contracting Officer Representative (COR): The COR will be identified by separate letter. The COR monitors all technical aspects of the contract and assists in contract administration. The COR is authorized to perform the following functions: assure that the Contractor performs the technical requirements of the contract: perform inspections necessary in connection with contract performance; maintain written and oral communications with the Contractor concerning technical aspects of the contract; issue written interpretations of technical requirements, including Government drawings, designs, specifications; monitor Contractor's performance and notifies both the Contracting Officer and Contractor of any deficiencies; coordinate availability of government furnished property, and provide site entry of Contractor personnel. A letter of designation issued to the COR, a copy of which is sent to the Contractor, states the responsibilities and limitations of the COR, especially with regard to changes in cost or price, estimates or changes in delivery dates. The COR is not authorized to change any of the terms and conditions of the resulting order.

1.6.12. Key Personnel: The follow personnel are considered key personnel by the government: Network Operations Manager, Network Engineer Level 2 (2), Network Engineer Level 3 (2), Voice Engineer Level 2 (2), Voice Engineer Level 3, VMWare Administrator, VMWare Engineer, Satellite Network Engineer Level 2 (1), and Satellite Network Engineer Level 3.

1.6.13. Identification of Contractor Employees: All contract personnel attending meetings, answering Government telephones, and working in other situations where their contractor status is not obvious to third parties are required to identify themselves as such to avoid creating an impression in the minds of members of the public that they are Government officials. They must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is

appropriately disclosed. All contract personnel will be required to obtain and wear the company's badge in the performance of this service.

1.6.14. Contractor Travel:

1.6.14.1. Contractor may be required to travel CONUS and OCONUS, if applicable, during the performance of this contract to attend meetings, conferences, training, or conduct engineering upgrades or implementations.

Estimate travel costs, based on historical data will be approximately $24,093.08 for the six (6) month period of performance.

1.6.14.2. Contractor will be authorized travel expenses consistent with the substantive provisions of the Joint Travel Regulation (JTR) and the limitation of funds specified in this contract. All travel requires Government approval/authorization and notification to the COR. Due to unforeseen mission requirements, the government will include a lump sum Travel CLIN to cover the unexpected travel costs.

1.6.14.3. Letter of Authorization (LOA): The contractor is responsible for mobilizing and demobilizing its workforce, including subcontractor employees. The Contracting Officer has the authority to extend selected LOAs up to, but not exceeding 30 calendar days after the contract completion date to allow the prime contractor to complete demobilization of its workforce and contractor owned equipment, as well as subcontractor(s) workforce and owned equipment.

1.6.14.4. Synchronized Pre-deployment Operational Tracker (SPOT): The contractor is responsible to initiate and close out deployment of personnel, including subcontractor employees, upon completion of travel release the personnel from the SPOT database. The release of employee information must be accomplished no more than 30 calendar days after the mission completion date.

1.6.15. Other Direct Costs This category includes miscellaneous expenses that may occur during travel and short notice work requirements. Defense Base Act (DBA) insurance is authorized.

1.6.16. Data Rights: The Government has unlimited rights to all documents/material produced under this contract. All documents and materials, to include the source codes of any software, produced under this contract shall be Government owned and are the property of the Government with all rights and privileges of ownership/copyright belonging exclusively to the Government. These documents and materials may not be used or sold by the contractor without written permission from the Contracting Officer. All materials supplied to the Government shall be the sole property of the Government and may not be used for any other purpose. This right does not abrogate any other Government rights.

1.6.17. Organizational Conflict of Interest: Contractor and subcontractor personnel performing work under this contract may receive, have access to or participate in the development of proprietary or source selection information (e.g., cost or pricing information, budget information or analyses, specifications or work statements, etc.) or perform evaluation services which may create a current or subsequent Organizational Conflict of Interests (OCI) as defined in FAR Subpart 9.5. The Contractor shall notify the Contracting Officer immediately whenever it becomes aware that such access or participation may result in any actual or potential OCI and shall promptly submit a plan to the Contracting Officer to

avoid or mitigate any such OCI. The Contractor's mitigation plan will be determined to be acceptable solely at the discretion of the Contracting Officer and in the event the Contracting Officer unilaterally determines that any such OCI cannot be satisfactorily avoided or mitigated, the Contracting Officer may affect other remedies as he or she deems necessary, including prohibiting the Contractor from participation in subsequent contracted requirements which may be affected by the OCI.

1.6.18. PHASE IN of Contractors in Place: To minimize any decreases in productivity and to prevent possible negative impacts on additional services, the Contractor shall have personnel on board within 15 days of the award.

Part 2
Qualifications

The workload projection of total labor categories (to include *CERTIFICATIONS, EDUCATION, EXPERIENCE, SKILLS, and CLEARANCE) is included and provided to indicate the Government's projection and the current staffing level to ensure successful performance. The workload projection is not intended to be binding on either party or to be the only possible solution to the requirement*.

2. Special Qualifications

REQUIREMENT	CERTIFICATIONS	EDUCATION	EXPERIENCE	SKILLS	CLEARANCE
Network Operations Manager (1) 3.1	CCNA CISSP	Bachelors' Degree in a Computer Science or relevant field OR Masters' Degree in Computer Science OR relevant field	8 years with Bachelors' Degree 5 years with Masters' Degree and 5 years with Net Manager experience	Ability to develop and implement network security policy; familiar with virtualization/cloud architectures; PKI knowledge, ITIL and Cisco ASRs, routers, switches, VPNs and VLANs.	TOP SECRET
Network Systems Manager (1)	MCSE VCP CISSP	Bachelor's Degree in a Computer Science OR relevant field	8 years with Bachelors' Degree OR 5 years with	Experience operating and configuring Windows Systems for enterprise architecture;	TOP SECRET

3.2		OR Masters' Degree in Computer Science OR relevant field	Masters' Degree and 5 years as Network Manager	remote management and server maintenance; DNS, WINS, DHCP, VMware, HBSS, SharePoint, SCCM; tactical data services administration; NET App and Cisco VCS; Understand Flexpad Architecture	
Network Engineer Level 2 (3) 3.3	CCNA AND SEC+	Bachelors' Degree in Computer Science or related field OR Masters' Degree in Computer Science or relevant field	5 years with Bachelors' Degree OR 4 years with Masters' Degree OR If no degree, 10 years direct work experience	Knowledge to use hardware/software tools to correct network issues; Experience with TCP/IP protocol stacks, wireless architectures and VoIP; In depth knowledge on data, voice, and video networks; Configure Cisco routers/switches, firewalls, VLANs, MPLS, OSPF, BGP, EIGRP, and QOS; NET APP, IOS-XR software, Cisco Unified Communications Manager and Cisco Unity	TOP SECRET

Network Engineer Level 3 (4) 3.4	CCNP Switching and Routing AND SEC+	Bachelors' Degree in Computer Science or related field OR Masters' Degree in Computer Science or relevant field	5 years performing Network/Voice engineering with Bachelors' Degree OR 4 years' experience working in Network/Voice Engineering with Masters' Degree	Knowledge to use hardware/software tools to correct network issues; Experience with TCP/IP protocol stacks, wireless architectures and VoIP; In depth knowledge on data, voice, and video networks; Configure Cisco routers/switches, firewalls, VLANs, MPLS, OSPF, BGP, EIGRP, and QOS; NET APP, IOS-XR software, Cisco Unified Communications Manager and Cisco Unity	TOP SECRET
Voice Engineer Level 2 (3) 3.5	CCNA Voice OR CCNA Collaboration AND SEC+ OR Equivalent	Bachelors' Degree in a Computer Science OR relevant field OR Masters' Degree in Computer Science or relevant field	5 years performing Network/Voice engineering with Bachelors' Degree OR Four years' experience working in Network/Voice Engineering with Masters'	Config knowledge of CM, UCS, CUPS, SBC, PG, AS/5400 Gateways, Unity Voicemail and SIP Trunks; multi-tiered Cisco IP apps; experience designing and implementing Cisco Networks, ISR routers, Analog Gateways, voice trunks, E1/T1	TOP SECRET

			Degree OR If no degree, 10 years direct work experience	(CAS,CCS) FXS/FXO, SIP Proxy, CUBE, AS-SIP, MGCP, SCCP, QOS configs, and LLQ; DISN voice network, UCR; develop and implement voice network diagrams	
Voice Engineer Level 3 (1) 3.6	CCNP Voice OR CCNP Collaboration AND SEC+ OR Equivalent	Bachelor's Degree in a Computer Science OR relevant field OR Masters' Degree in Computer Science OR relevant field	8 years performing Network/Voice engineering with Bachelors' Degree OR 4 years' experience working in Network/Voice Engineering with Masters' Degree	SME in UC, Network admin; troubleshooting data and voice networks; analytical and problem-solving skills, Time Management Skills; Excellent Planning and Organizing Skills; experience with CM configurations ,UCS, CUPS, SBC, PG, AS/5400 Gateways, Unity Voice Mail and SIP Trunks; multi-tiered Cisco IP and telephony apps; experience in Cisco IP telephony Networks; Demonstrate knowledge VLAN, Voice VLAN, VTP, STP, PoE, Ether channel, HSRP, and multiple routing protocols; Cisco Voice Gateways (ISR Routers, ISR G2	TOP SECRET

				Routers and Analog gateways), voice trunks, E1/ T1(CAS,CCS), FXS /FXO, Gatekeepers, SIP Proxy , CUBE; Strong experience in DISN voice networks, IP theory; familiarity with RMF and its rules & regulations.	

VMWare Administrator Level 2 (2) 3.7	VMWare Certified Associate 5/6 - Data Center Virtualization AND SEC+	Bachelors ’Degree in IT or related field	8 years in IT within a VMWare environment OR 7 years' experience working in an IT environment (instead of degree)	Experience with MS server 2008 and newer; MS Active Directory, Group Policies, MS Office SQL 2005 and newer, IIS 6.0 and newer, VMWare, VMWare View and Windows 7 and newer; Experience with ThinApp technology.	TOP SECRET
VMWare Engineer Level 3 (1) 3.8	VMWare Certified Professional 5/6 - Data Center Virtualization AND SEC+	Bachelors’ Degree in IT or related field OR Master’s Degree in IT or related field	8 years in IT within a VMWare environment OR 4 years with a Master’s Degree	Experience with Windows MS Server 2008/2012, performance tuning, recovery testing Build, run scripts(PowerShell); Hands on experience with Windows Active Directory, Exchange Server, VMware environments, Enterprise windows servers, TCP/IP based services, DNS, DHCP, HTTP, FTP, SSH, and SMTP.	TOP SECRET
Satellite Network Engineer Level	CCNA Switching and Routing; AND	Bachelors’ Degree in a Computer	Five years satellite network	Strong knowledge in configuration, training, testing,	TOP SECRET

2 (3) 3.9	SEC+ OR equivalent AND Certified iGT Installer/Operator/Maintainer	Science OR relevant field OR Masters' Degree in Computer Science OR relevant field	engineering experience with Bachelors' Degree OR Four years' satellite network engineering experience with Masters' Degree OR 10 years direct work experience instead of degree; Must be trained in a DoD satellite related field	operation, testing, fielding, installation and maintenance of SATCOM networks and systems; TDMA, MF-TDMA, FDMA; deploy tactical/strategic systems and subsystems; documented experience in SATCOM architecture; analysis of iDirect, ViaSat, L3, Tampa Microwave, Windmill, DRS SCOSS-J, and GD, VSAT; familiarity with RMF and its rules & regulations.	

Satellite Network Engineer Level 3 (1) 3.10	CCNA Switching and Routing or equivalent; AND SEC+ or equivalent AND Certified iGT, Advance Installer/Operator/Maintainer	Bachelors' Degree in a Computer Science OR relevant field OR Masters' Degree in Computer Science OR relevant field	5 years satellite network engineering experience with Bachelors' OR 4 years satellite network engineering experience with Masters' Degree	Knowledge in configuration, training, testing, operation, fielding, installation and maintenance of SATCOM networks/systems; TDMA, MF-TDMA, FDMA; troubleshoot tactical & strategic SATCOM systems and subsystems; document SATCOM architecture; demonstrate skills in configuration, implementation, and analysis of SATCOM systems to include, iDirect, ViaSat, L3, Tampa Microwave, Windmill, DRS SCOSS-J, GD, VSAT. IP theory and demonstrated packet switching and routing concepts; familiarity with risk management framework (RMF) and its rules & regulations.	TOP SECRET

Waivers of any education, experience, or certifications requirements are on a case by case basis and can only be waived by the J6 director.

3. PERFORMANCE TASKS

3.1. **NETWORK OPERATIONS MANAGER (one):** Shall function as the team lead, assisting the government in managing technical work quality, strategy and execution for the Enterprise Network Operations.

3.1.1. DUTIES:

3.1.1.1. Provide support to deployed tactical users accessing managed DISN-TE sites, architecture, and services including data, transmission, voice, video, and any interoperability/connectivity support requirements tactical users' encounter.

3.1.1.2. Provide recommendations to Government leadership on technology investments, engineering change proposals, technology migration strategies, and network design changes.

3.1.1.3. Develop system and sub-component technical requirements for operational requirements.

3.1.1.4. Assess network designs, conduct network packet traffic analyses, perform network capacity planning and network security vulnerabilities.

3.1.1.5. Configure locally and remotely manage devices such as routers and switches, Cisco Unified Communications Managers, network accelerators, firewalls, packet encryptors and servers.

3.1.1.6. Provide engineering support for classified and unclassified information systems to include developing system documentation, performing traffic analysis, and monitoring system and component operational availability (i.e. uptime).

3.1.1.7. Configure boundary protection for JCSE networks and service enclaves by implementing and documenting the design of firewalls, proxy servers, and intrusion detection/protection capabilities.

3.1.1.8. Provide Telephony Systems engineering support to evaluate, document, install, operate, configure, and maintain various COTS voice systems to include Cisco Unified Communications Managers, Integrated Gateway Exchange (IGX) switches, and various other telephony devices.

3.1.1.9. Manage incident and problem management to include recording, classification and initial response, investigation and diagnosis, resolution, recovery, and incident closure.

3.1.1.10. Ensure proper systems administration is performed for supported networks.

3.1.1.11. Ensure proper operations, maintain, upgrade, and implementation of local area networks (LAN) and wide area networks (WAN).

3.1.1.12. Develop and maintain systems, network, and architectural artifacts.

3.1.1.13. Manage physical network infrastructure to include Government Furnish Equipment (GFE) cable installation, testing, troubleshooting and management for IP voice, secure IP voice, and IP video.

3.1.1.14. Provide configuration management to include managing the Master Station log and administrative logs, documentation and software configuration inventory, hardware inventory tracking, and status accounting processes.

3.1.1.15. Participate in technical exchange meetings and configuration/change management boards when requested by the Government. Produce documentation to reflect results of technical exchange meetings and configuration/change management boards to define IT configuration items.

3.1.1.16. Analyze information assurance-related technical problems and provide engineering support in solving these problems.

3.1.1.17. Ensure compliance with: DoDI 8510.01, Risk Management Framework for DoD IT; DoDD 8570.01, Information Assurance Training, Certifications and Workforce Management; DoDD 8140.01 Cyberspace Workspace Management; DoDI 8320.07 Implementing the Sharing of Data, Information and IT Services in DoD; JCSE Technical Management Guide; and JCSE Instruction 10-13, Network Operations as they pertaining to the unit's systems/networks.

3.1.1.18. Properly notify the government when changes to DoDI 8510.01, Risk Management Framework for DoD IT; DoDD 8570.01, Information Assurance Training, Certifications and Workforce Management; DoDD 8140.01 Cyberspace Workspace Management; DoDI 8320.07 Implementing the Sharing of Data, Information and IT Services in DoD; JCSE Technical Management Guide; and JCSE Instruction 10-13, Network Operations impact the unit's systems/networks.

3.1.1.19. Provide technical support to the IA Cell to develop and maintain JCSE IA processes and procedures regarding JCSE's computer network defense in-depth protection for the JCSE enterprise.

3.1.1.20. Perform and support updates to and maintenance of the POA&Ms for the JCSE Enterprise.

3.1.1.21. Support to development of RMF Security Plans.

3.1.1.22. Document changes to systems and all required checklists for use within the JCSE Enterprise.

3.1.1.23. Periodically review the JCSE Enterprise architecture to ensure compliance with DoD guidance and direction.

3.1.1.24. Implement and integrate IA defense postures to JCSE's Enterprise systems and architectures when coordinated or immediately upon being directed to secure reported cyber threats from the appropriate level of authority.

3.2. NETWORK SYSTEMS MANAGER (one):

3.2.1. DUTIES: Function as team lead to provide tier level 2/3 support to deployed tactical users accessing JCSE managed DISN-TE sites, architecture, and services including data, transmission, voice, video, and any interoperability/connectivity support requirements tactical users' encounter.

3.2.1.1. Shall provide tier level 2/3 support to users accessing JCSE managed Enterprise including DISN-TE sites, architecture, and services including data, transmission, voice, video, and any interoperability/connectivity support requirements users' encounter.

3.2.1.2. Develop system and sub-component technical requirements for validated operational requirements.

3.2.1.3. Provide engineering support in solving information assurance-related technical problems.

3.2.1.4. Comply with DoDI 8510.01, Risk Management Framework for DoD IT; DoDD 8570.01, Information Assurance Training, Certifications and Workforce Management; DoDD 8140.01 Cyberspace Workspace Management; DoDI 8320.07 Implementing the Sharing of Data, Information and IT Services in DoD; JCSE Technical Management

Guide; and JCSE Instruction 10-13, Network Operations as they pertaining to the unit's systems/networks.

3.2.1.5. Lead the technical team that is responsible for installing, configuring, and, maintaining operating system workstations and servers, including web servers, in support of business processing requirements.

3.2.1.6. Perform software installations and upgrades to operations system and software packages.

3.2.1.7. Evaluate, implement, and manage appropriate software and hardware solutions to ensure workstation/server data integrity.

3.2.1.8. Implement a schedule of system backups, restorals, and database archive operations to ensure data/media recoverability.

3.2.1.9. Develops and promotes standard operating procedures.

3.2.1.10. Conducts routine hardware and software audits of workstations and servers to ensure compliance with established standards, policies, and configuration guidelines.

3.2.1.11. Develops and maintains a comprehensive operating system hardware and software configuration database/library of all supporting documentation.

3.2.1.12. Configure, administer and maintain Windows servers (2008,2012, and 2016), Active Directory, Microsoft Terminal servers and other Microsoft services including DNS, DHCP, File, and Print.

3.2.1.13. Ensure operations and maintenance of SAN (Storage Area Network) technology, blade server technology (to include Dell and Cisco UCS systems) and backup server technology.

3.2.1.14. Configure servers to provide required levels of access, reliability and availability.

3.2.1.15. Ensure hosts, virtual machines, and the virtual center are compliant with all security and performance guidance and are properly maintained.

3.2.1.16. Ensure all virtual machines have sufficient resources to perform daily processes.

3.2.1.17. Ensure creation and administration of virtual or physical test networks to include coordinating tasks with the team's SharePoint developers and engineers.

3.2.1.18. Perform systems integration functions on the server farms involving software products (GOTS or COTS) that provide additional SharePoint artifacts (i.e., Web Parts, Templates, Master Pages, etc.).

3.2.1.19. Document and publish knowledge regarding best practices or solutions; documents must be consistent with JCSE’s enterprise level portal related initiatives (i.e. federated search).

3.2.1.20. Participate in technical exchange meetings, reviews and configuration/change management boards when requested by the Government. Document results of technical exchange meetings and configuration/change board meetings to define IT configuration items.

3.2.1.21. Lead technical efforts to build and deploy servers and supporting applications.

3.2.1.22. Properly notify the government when changes to DoDI 8510.01, Risk Management Framework for DoD IT; DoDD 8570.01, Information Assurance Training, Certifications and Workforce Management; DoDD 8140.01 Cyberspace Workspace Management; DoDI 8320.07 Implementing the Sharing of Data, Information and IT

Services in DoD; JCSE Technical Management Guide; and JCSE Instruction 10-13, Network Operations impact the unit's systems/networks.

3.2.1.23. Perform and support updates to and maintenance of the POA&Ms for the JCSE Enterprise.

3.2.1.24. Support to development of RMF Security Plans.

3.2.1.25. Document changes to systems and all required checklists for use within the JCSE Enterprise.

3.2.1.26. Periodically review the JCSE Enterprise architecture to ensure compliance with DoD guidance and direction.

3.2.1.27. Implement and integrate IA defense postures to JCSE's Enterprise systems and architectures when coordinated or immediately upon being directed to secure reported cyber threats from the appropriate level of authority.

3.3. Network Engineer Level II (Three 24/7 Shift Workers):

3.3.1. DUTIES:

3.3.1.1. Provide Enterprise (including tactical) data network engineering support to plan, evaluate, document, install, configure, operate, maintain, and conduct operational management, configuration, and troubleshooting for onsite and remote access to all managed COTS-based products.

3.3.1.2. Provide engineering support for daily operations and maintenance of a multi-vendor telecommunications infrastructure that includes Cisco routers and switches, Cisco Unified Communications Managers, Riverbed network accelerators, multiple vendor firewalls, and multiple vendor products.

3.3.1.3. Ensure the secure and reliable operation of JCSE’s enterprise data networks to provide maximum performance and availability for system users.

3.3.1.4. Provide engineering support for designing, installing, maintaining and supporting current and future LAN, WAN and VoIP infrastructures. Engineering support includes data, voice, and video network technology development, integration, configuration, testing, and deployment.

3.3.1.5. Provide technical support for data networks to include, creation and maintenance of network technical documentation.

3.3.1.6. Develop plans to upgrade network components, processes and operating procedures identified by the Government.

3.3.1.7. Provide operation and maintenance, advanced engineering and administration of multi-protocol routers, multi-layer switches, network security devices and network management systems.

3.3.1.8. Install, configure, and operate data, voice, and video telecommunications equipment.

3.3.1.9. Provide engineering support for data network issues impacting DISN-TE sites.

3.3.1.10. Analyze information assurance-related technical problems and provide engineering support in solving these problems.

3.3.1.11. Ensure compliance with DoDI 8510.01, Risk Management Framework for DoD IT; DoDD 8570.01, Information Assurance Training, Certifications and Workforce Management; DoDD 8140.01 Cyberspace Workspace Management; DoDI 8320.07

Implementing the Sharing of Data, Information and IT Services in DoD; JCSE Technical Management Guide; and JCSE Instruction 10-13, Network Operations as they pertain to the unit's systems/networks.

3.3.1.12. Properly notify the government when changes to DoDI 8510.01, Risk Management Framework for DoD IT; DoDD 8570.01, Information Assurance Training, Certifications and Workforce Management; DoDD 8140.01 Cyberspace Workspace Management; DoDI 8320.07 Implementing the Sharing of Data, Information and IT Services in DoD; JCSE Technical Management Guide; and JCSE Instruction 10-13, Network Operations impact the unit's systems/networks.

3.3.1.13. Provide technical support the vulnerability and risk analyses of computer systems and applications during all phases of the system development life cycle.

3.3.1.14. Provide technical support to the IA Cell to develop and maintain JCSE IA processes and procedures regarding JCSE's computer network defense in-depth protection for the JCSE enterprise.

3.3.1.15. Perform and support updates to and maintenance of the POA&Ms for the JCSE Enterprise.

3.3.1.16. Support development of RMF Security Plans.

3.3.1.17. Document changes to systems and all required checklists for use within the JCSE Enterprise.

3.3.1.18. Periodically review the JCSE Enterprise architecture to ensure compliance with DoD guidance and direction.

3.3.1.19. Implement and integrate IA defense postures to JCSE's Enterprise systems and architectures when coordinated or immediately upon being directed to secure reported cyber threats from the appropriate level of authority.

3.4. NETWORK ENGINEER LEVEL III (Four 24/7 Shift Workers):

3.4.1. DUTIES:

3.4.1.1. Perform all duties of Tier 2 network engineer identified in this PWS.

3.4.1.2. Develop network design and optimization plans to resolve complex performance, security, reliability and availability deficiencies or problems.

3.4.1.3. Advise Government leadership regarding the enterprise-level impacts of implementing new technology or equipment in the JCSE network.

3.4.1.4. Make recommendations regarding the evolution of the overall network architecture.

3.4.1.5. Perform root cause analysis of incidents and problems; develop solutions that prevent the incident or problem from recurring.

3.4.1.6. Identify system architecture issues or methodologies that must be corrected to prevent further incidents from recurring.

3.4.1.7. Perform proactive analysis and trend analysis to identify and resolve problems before they occur.

3.4.1.8. Investigate diagnosis and perform root cause analysis for enterprise level network problems.

3.4.1.9. Develop solutions consistent with JCSE’s change/configuration management processes for enterprise level problems.

3.4.1.10. Communicate with service providers and other non-JCSE entities as needed to troubleshoot, isolate and analyze complex issues or problems.

3.4.1.11. Participate in Configuration Control Board (CCB) meetings and technical exchange meetings when requested by the Government.

3.4.1.12. Research, evaluate and recommend solutions to ensure that JCSE's networks retain the highest possible degree of security, reliability, availability and performance.

3.4.1.13. Perform detailed research of best industry practices and leading-edge solutions to JCSE's future capability requirements as identified by the Government.

3.4.1.14. Perform analysis of alternatives for solutions to complex, persistent network problems in the current architecture or anticipated in future architecture.

3.4.1.15. Develop and provide documentation and implementation plans for upgrades and new capabilities.

3.5. VOICE ENGINEER LEVEL II (Three 24/7 Shift Workers):

3.5.1. DUTIES:

3.5.1.1. Develop solutions for Enterprise voice and collaboration network architecture.

3.5.1.2. Ensure telecommunications services are in compliance with the DoD's Unified Capabilities Requirement (UCR) and applicable Information Assurance regulations and instructions.

3.5.1.3. Identify voice network requirements and provide technical support for the analysis, acquisition, installation and operation of voice network hardware and software components.

3.5.1.4. Provide telephony systems engineering support to evaluate, document, install, operate, and maintain commercial-off-the-shelf (COTS) voice systems to include Cisco Unified Communications Managers, Integrated Gateway Exchange (IGX) switches, HAIPE encryption devices, and other devices that are part of the JCSE voice network.

3.5.1.5. Act as technical lead for implementation of IP telephony, unified messaging, and voice technologies on all segments of the JCSE voice enterprise network.

3.5.1.6. Collaborate closely with technical teams and work groups to develop and implement secure and sustainable solutions to telephony and collaboration requirements for deployed tactical kit operations and tactical solutions.

3.5.1.7. Implement, maintain and support centralized telecommunications infrastructure specializing in UC (Unified Communications), including systems administration, troubleshooting, analysis, testing, research, provisioning, training, problem solving, technical support, development, and testing/deployment of new applications, hardware, and systems.

3.5.1.8. Document voice networks to include user support processes and standard operating procedures.

3.5.1.9. Perform hardware and software maintenance for voice network components to include information assurance updates on telephony systems.

3.5.1.10. Participate as a voice network subject matter expert (SME) in designated work groups and tiger teams addressing the installation, configuration, troubleshooting,

and monitoring of core LAN/WAN services required for VoIP (Voice Over Internet Protocol) deployments including QOS (Quality of Service), COS (Class Of Service) VLANs (Virtual Local Area Network), SBCs (Session Border Controller) and SIP (Session Initiated Protocol) Carrier Services.

3.5.1.11. Monitor and analyze network quality and operational processes and follow-up with the appropriate corrective/preventative action plans.

3.5.1.12. Coordinate with the Cisco TAC in order to resolve IOS/IOS XE bugs, Software defects, configuration errors, and/or issues impacting performance of the JCSE architecture.

3.5.1.13. Interpret network alert and performance management tool output to properly engineer the capacity and resiliency of the UC (Unified Communications) portion of the VoIP network.

3.5.1.14. Implement Cisco IP Telephony solutions and project plans thru implementation of Cisco Unified Communications applications including Cisco Unified Communications Manager, Unity, Unified Communications Manager Express, Meeting Place, VOIP and TDM physical services.

3.5.1.15. Support integration of voice systems with UC video.

3.5.1.16. Support unique requirements and challenges of providing service in low bandwidth and austere environments.

3.5.1.17. Properly notify the government when changes to DoDI 8510.01, Risk Management Framework for DoD IT; DoDD 8570.01, Information Assurance Training, Certifications and Workforce Management; DoDD 8140.01 Cyberspace Workspace Management; DoDI 8320.07 Implementing the Sharing of Data, Information and IT Services in DoD; JCSE Technical Management Guide; and JCSE Instruction 10-13, Network Operations impact the unit's systems/networks.

3.5.1.18. Perform vulnerability and risk analyses of voice systems and applications.

3.5.1.19. Provide technical support to the IA Cell to develop and maintain JCSE IA processes and procedures regarding JCSE's voice network defense in-depth protection.

3.5.1.20. Perform and support updates to and maintenance of the POA&Ms applicable to voice components of the JCSE Enterprise.

3.5.1.21. Support to development of RMF Security Plans.

3.5.1.22. Document changes to voice systems and all required checklists for use within the JCSE Enterprise.

3.5.1.23. Periodically review the JCSE Enterprise architecture to ensure compliance of voice components with DoD guidance and direction.

3.6. VOICE ENGINEER LEVEL III (One):

3.6.1. DUTIES:

3.6.1.1. Perform all duties of Tier 2 voice engineer identified in this PWS.

3.6.1.2. Develop voice network design and optimization plans to resolve complex performance, security, reliability and availability deficiencies or problems.

3.6.1.3. Make recommendations regarding the evolution of JCSE’s voice network architecture.

3.6.1.4. Perform root cause analysis of incidents and problems on the voice network; develop solutions that prevent the incident or problem from recurring.

3.6.1.5. Identify voice system architecture issues or methodologies that must be corrected to prevent further incidents from recurring.

3.6.1.6. Perform proactive analysis and trend analysis to identify and resolve problems before they occur.

3.6.1.7. Investigate, diagnosis, and perform root cause analysis for voice network problems.

3.6.1.8. Develop solutions consistent with JCSE's change/configuration management processes for voice network problems.

3.6.1.9. Communicate with service providers and other non-JCSE entities as needed to troubleshoot, isolate and analyze complex issues or problems on the JCSE voice network.

3.6.1.10. Participate in Configuration Control Board (CCB) meetings and technical exchange meetings when requested by the Government.

3.6.1.11. Research, evaluate and recommend solutions to ensure that JCSE's voice networks retain the highest possible degree of security, reliability, availability and performance.

3.6.1.12. Perform detailed research of best industry practices and leading-edge solutions to JCSE's future voice network capability requirements as identified by the Government.

3.6.1.13. Perform analysis of alternatives for solutions to complex, persistent voice network problems in the current architecture or anticipated in future architecture.

3.7. VMWare ADMINISTRATOR LEVEL II (Two 24/7 Shift Workers):

3.7.1. DUTIES

3.7.1.1. Shall have knowledge of DoD and Joint Service computer network and communications regulations, services and instructions to ensure computer systems and telecommunications services are in compliance with applicable information assurance regulations and instructions

3.7.1.2. The contractor shall ensure that adequate and appropriate planning is provided for remote hardware and communications facilities to develop and implement methodologies for analysis, installation and support of data center virtualization.

3.7.1.3. The contractor shall provide coordination in the analysis, acquisition, and installation of remote hardware and software.

3.7.1.4. Position requires network engineer to consistently work current architecture, but also support future and bleeding/leading edge technologies that enhance or will enhance JCSE's enterprise data, voice, and video network architectures.

3.7.1.5. The contractor shall be responsible for documentation including support processes and operating procedures.

3.7.1.6. The contractor shall have familiarity with RMF, write parts of POA&M, continually update SSP

3.7.1.7. The contractor shall engage in hands-on lab testing and development for problem resolution, new product reporting, or technical functionality. Review

application of STIGs and DOD configuration guidance in images for completeness and correctness.

3.7.1.8. The contractor shall write documentation in regards to administration, maintenance, structure, and user permissions for servers.

3.7.1.9.

3.7.1.10. The contractor is responsible for implementing, tuning and maintaining VMware based solutions, implements VMware vSphere for server consolidation and virtualization and actively seeks out opportunities to improve existing practices, procedures, and technology implementations also applies technical knowledge of networks, operating systems, utilities, etc. to the VMware environment.

3.7.1.11. The contractor shall have ability to perform root cause analysis on all VMware products. E.g. ESX hosts, Virtual Centers, and Virtual Machines.

3.7.1.12. The contractor shall have the ability to administer, maintain, and troubleshoot Storage Area Networks (SAN) and Network Attached Storage (NAS) attached to VMware environments

3.7.1.13. The contractor shall provide Tier 2 support to an enterprise operations center with local and forward deployed VMWare environments.

3.8. VMWare ENGINEER LEVEL III (One):

3.8.1. DUTIES

3.8.1.1. Perform all duties of Tier 2 VMWare engineer identified in this PWS.

3.8.1.2. The contractor shall be able to troubleshoot, isolate and identify problems with all servers to include Microsoft (MS) SharePoint, MS Domain Controller (DC), MS Exchange, VMWare VIEW VDI, VMWare vCenter, MS SQL, MS Client Access Server/Hub Transport Server, MS Exchange Mailbox Store, Cisco Unity Connection, UCS, NetApps, CUCM, DNS, Print Management, MS System Center Configuration Manager (SCCM), MS Windows Deployment Services Server, network management and monitoring suites such as WhatsUp Gold or Spectrum, ACAS (Nessus and Passive Vulnerability Scanner) along with corresponding NetApp SAN, NAS, and other server or storage solutions The contractor shall ensure that adequate and appropriate planning is provided for remote hardware and communications facilities to develop and implement methodologies for analysis, installation and support of data center virtualization.

3.8.1.3. The contractor shall acquire, configure and maintain development, test and production servers in the physical and virtual environment.

3.8.1.4. The contractor shall provide technical and procedural direction to JCSE for the implementation of the network servers used, as well as interface with internal users, development personnel and other technical staff

3.8.1.5. The contractor shall provide direction in complex problem solving situations and participate in direct interaction with internal staff as required. Identify process improvement opportunities achievable through the optimum use of the servers. The contractor is responsible for implementing, tuning and maintaining VMware based solutions, implements VMware vSphere for server consolidation and virtualization and actively seeks out opportunities to improve existing practices, procedures, and

technology implementations also applies technical knowledge of networks, operating systems, utilities, etc. to the VMware environment.

3.8.1.6. The contractor shall have the ability to build and maintain the servers required for development work, internal testing, customer testing and production environments. Maintain file version consistency across all development servers. Maintain access privileges and account groups as directed by development team.

3.8.1.7. The contractor shall have the ability to design, implement, and maintain a consistent backup and disaster recovery plan.

3.8.1.8. The contractor shall document technical requirements, develop and oversee project plans and implement change control procedures.

3.8.1.9. The contractor shall collaborate with operations, QA and third party data centers to provide technical direction on network topologies, server configurations, hardware/software deployments, firewall configurations and other administrative tasks related to the staging and maintenance of company development, testing and production servers.

3.9. SATELLITE NETWORK ENGINEER LEVEL II (Three 24/7 Shift Workers):

3.9.1. DUTIES:

3.9.1.1. Develop methodology and implementation strategies for optimizing the performance, security, reliability and availability of JCSE's SATCOM systems.

3.9.1.2. Provide engineering support for the implementation of a multiple hub, terrestrially connected global network.

3.9.1.3. Support engineering efforts of planning and performance management, maintenance, enhancements, upgrades, and integration support of other SATCOM hardware and software systems and subsystems.

3.9.1.4. Provide daily operational support, to include troubleshooting and problem resolution for SATCOM systems as necessary to support JCSE's global networks.

3.9.1.5. Assist with development of on-site network operations familiarization training, development of methodology and implementation strategies for SATCOM systems, network design, and system hardware and software documentation.

3.9.1.6. Monitor and report on the overall health of JCSE's satellite networks to include but not limited to, server memory, CPU, and hard disk usage, as well as, error, alarm, and warning responses and mitigation. Reports shall address network efficiency on bandwidth and timeslot usage, Quality of Service policies compliance, and findings on network audits. Reports shall identify specific areas of concern with recommendations for improvement.

3.9.1.7. Provide bandwidth usage reports to determine efficiency of satellite network performance and resource allocation.

3.9.1.8. Perform system and equipment integration in accordance with government-approved documentation, drawings, test plans, and procedures.

3.9.1.9. Validate baseline configurations and best practices specific to JCSE CONOPS for DISN-TE and deployable hubs.

3.9.1.10. Support engineering projects requiring SATCOM testing environments to include technical support for the networks to support test objectives.

3.9.1.11. Participate in Government-led testing consistent with designated test procedures on SATCOM communications systems for fixed, tactical, and mobile platforms.

3.9.1.12. Provide white papers, configuration guides, and other technical documentation to assist JCSE personnel and other DISN-TE community of interest members on equipment configurations and operations.

3.9.1.13. Provide technical support to JCSE maintenance team regarding satellite equipment faults.

3.9.1.14. Provide input for SATCOM configurations regarding future plans/upgrade/installs.

3.9.1.15. Address redundancy and failover implementation of all satellite networks to include database backup, line card redundancy, and protocol processor load balancing.

3.9.1.16. Develop satellite system hardware and software documentation, including system operator manuals, equipment maintenance manuals, operator guides, and operating system software.

3.9.1.17. Develop documentation on testing and evaluation of modem and antenna equipment for JCSE modernization.

3.9.1.18. Analyze information assurance-related technical problems on JCSE's satellite networks and provide engineering support in solving these problems.

3.9.1.19. Ensure compliance with DoDI 8510.01, Risk Management Framework for DoD IT; DoDD 8570.01, Information Assurance Training, Certifications and Workforce Management; DoDD 8140.01 Cyberspace Workspace Management; DoDI 8320.07 Implementing the Sharing of Data, Information and IT Services in DoD; JCSE Technical Management Guide; and JCSE Instruction 10-13, Network Operations as they pertaining to JCSE's satellite systems/networks.

3.9.1.20. Notify the government when changes to DoDI 8510.01, Risk Management Framework for DoD IT; DoDD 8570.01, Information Assurance Training, Certifications and Workforce Management; DoDD 8140.01 Cyberspace Workspace Management; DoDI 8320.07 Implementing the Sharing of Data, Information and IT Services in DoD; JCSE Technical Management Guide; and JCSE Instruction 10-13, Network Operations impact JCSE's satellite systems/networks.

3.9.1.21. Perform vulnerability and risk analyses of satellite systems and applications.

3.9.1.22. Provide technical support to the IA Cell to develop and maintain JCSE IA processes and procedures regarding satellite network and components that are part of the JCSE enterprise.

3.9.1.23. The contractor shall provide technical support to the updates to, and maintenance of, POA&Ms addressing satellite equipment and components of the JCSE Enterprise.

3.9.1.24. Support to development of RMF Security Plans covering the satellite network equipment and components that are part of the JCSE enterprise network.

3.9.1.25. Document changes to satellite equipment and systems and all required checklists for use within the JCSE Enterprise.

3.9.1.26. Periodically review the satellite network segment of the JCSE Enterprise architecture to ensure compliance with DoD guidance and direction.

3.9.1.27. Implement and integrate IA defense postures for the satellite network segment of JCSE's Enterprise systems and architectures when coordinated or immediately upon being directed to secure reported cyber threats from the appropriate level of authority.

3.10. SATELLITE NETWORK ENGINEER LEVEL III (One 24/7 Shift Workers):

3.10.1. DUTIES:

3.10.1.1. Be capable of performing all duties of Tier 2 network engineer identified in this PWS when requested by the Government.

3.10.1.2. Develop satellite network design and optimization plans to resolve complex performance, security, reliability and availability deficiencies or problems.

3.10.1.3. Advise Government leadership regarding the enterprise-level impacts of implementing new technology or equipment on the satellite network segment of JCSE's enterprise network.

3.10.1.4. Make recommendations regarding the evolution of the overall satellite network architecture.

3.10.1.5. Perform root cause analysis of incidents and problems identified on the satellite network or components; develop solutions that prevent the incident or problem from recurring.

3.10.1.6. Identify satellite network and system architecture issues or methodologies that must be corrected to prevent further incidents from recurring.

3.10.1.7. Perform proactive analysis and trend analysis to identify and resolve problems before they occur.

3.10.1.8. Investigate, diagnosis, and perform root cause analysis for enterprise level satellite network problems.

3.10.1.9. Develop solutions consistent with JCSE's change/configuration management processes for enterprise level problems.

3.10.1.10. Communicate with service providers and other non-JCSE entities as needed to troubleshoot, isolate and analyze complex issues or problems.

3.10.1.11. Participate in Configuration Control Board (CCB) meetings and technical exchange meetings when requested by the Government.

3.10.1.12. Research, evaluate and recommend solutions to ensure that JCSE's satellite networks retain the highest possible degree of security, reliability, availability and performance.

3.10.1.13. Perform detailed research of best industry practices and leading-edge solutions to JCSE's future satellite capability requirements as identified by the Government.

3.10.1.14. Perform analysis of alternatives for solutions to complex, persistent satellite network problems in the current architecture or anticipated in future architecture.

3.11 TIER-1 SERVICE DESK SUPPORT

3.11.1 Provides support to end users on a variety of issues. Identifies, researches, and resolves technical problems. Responds to telephone calls, email and personnel requests for technical support. Documents, tracks, and monitors the problem to ensure a timely resolution.

3.11.2 The contractor shall provide Tier 1 support to end users as the entry point for customers by receiving, recording, resolving and/or escalating requests for service.

3.11.3 Tier 1 specialists follow all documented processes and procedures related to call handling, call escalation, data capturing, closure and follow up procedures.

3.11.4 Provide support to end users focusing on operations, hardware, software, and network connectivity.

3.11.5 Specialist shall be responsible for communicating with customers to provide status, feedback, or general information regarding their request or inquiry for service.

3.11.6 Contractor shall provide support for system monitoring and system updates using procedures provided by Application Owners.

3.11.7 Contractor shall conduct customer satisfaction call backs via phone and/or email and record results in the incident tracking system.

3.11.8 The contractor shall monitor trends in problems and questions and seek opportunities to improve support and training processes.

3.11.9 Contractor shall simulate or recreate user problems to resolve operating system difficulties.

3.11.10 The contractor shall recommend systems modifications and upgrades to reduce user problems.

3.11.11 Contractor shall maintain technical proficiency and vast technical knowledge in field of expertise.

3.11.12 Shall escalate more complex problems to senior level for resolution.

3.11.13 The contractor shall image, configure and install computer systems and peripherals; provide applications analysis, review, evaluation, troubleshooting, integration, security, and maintenance support for the JCSE garrison LAN/WAN.

3.11.14 The contractor shall perform duties as follows:
Answer requests by the trouble-ticket Help Desk, telephone, or email for IT support.

- Assist with problem identification and resolution by assisting end users as the first and/or second level of support or by determining ecalation priority to the appropriate information

systems personnel.

- Assist with maintaining technical libraries and lessons learned documentation.
- Coordinate the repair of computers with users and other internal staff or with outside service repair technicians.
- Assist in the turn-in of outdated and/or inoperable automated data processing equipment (ADPE) to the Defense Reutilization and Marketing Office (DRMO).
- Develop knowledge and technical skills on a continuous basis to stay abreast of current trends and developments in information technology.
- Comply with all JCSE information security policies and directives.
- Mobile device setup configuring and troubleshooting.
- IT Asset management.
- Assist end users with audio visual requests.

3.12 **Tier-1 Helpdesk Support Required Skills and Abilities:**

3.12.1 Strong working knowledge of Microsoft operating systems, products, and applications, Remedy Service Desk, and hardware/software troubleshooting techniques.

3.12.2 Comfortable working with technology and applications.

3.12.3 Good inter-personal and communications skills. Meets with key staff members to address Help Desk issues within two hours of notification.

3.12.4 Good problem diagnosis and resolution skills.

3.12.5 Excellent attention to detail and follow-up skills.

3.12.6 Ability to work as a team player and provide professional customer service.

3.12.7 The Help Desk Analyst Support contractor requires a minimum of a current IAT II certification (GSEC or Security+CE or SSCP). Contractor must meet professional certification upon appointment.

3.12.8 Must have a minimum of 2 years' experience in IT customer support.

3.12.9 Contractor must have a Top Secret clearance.

3.13 TIER-2 SERVICE DESK / INCIDENT MANAGER

3.13.1 The Incident Manager is responsible for the effective implementation of the Incident Management process and carries out the corresponding reporting. They represent the first stage of escalation for incidents, should these not be resolvable within the agreed Service Levels. The Incident Manager develops and maintains the processes and procedures for incident management, incident escalation, and resolution teams. The Incident Manager is the lead technical manager for developing and documenting processes and reporting measures for incident resolution metrics. The Incident manager performs the screening and approval of knowledge management artifacts for incident management and service desk operations. As lead for the service desk, the Incident Manager maintains and verifies the skills qualifications and performance of all service desk staff.

3.13.2 Handles problems that the first-tier of help desk support is unable to resolve. May interact with network services, software systems engineering, and/or applications development to restore service and/or identify and correct core problem. Simulates or recreates user problems to resolve operating difficulties. Recommends systems modifications to reduce user problems. Maintains currency and high level of technical skill in field of expertise. Escalates more complex problems to senior level.

3.13.3 The contractor shall provide Tier II support to end users as the entry point for customers by receiving, recording, resolving and/or escalating requests for service.

3.13.4 The contractor shall follow all documented processes and procedures related to call handling, call escalation, data capturing, closure and follow up procedures.

3.13.5 The contractor shall be responsible for Communicating with customers to provide status, feedback, or general information regarding their request or inquiry for service.

3.13.6 The contractor shall provide support for system monitoring and system updates using procedures provided by Application owners.

3.13.7 The contractor shall conduct customer satisfaction call backs via phone and/or email and record results in the incident tracking system.

3.13.8 The contractor shall monitor trends in problems and questions and seek opportunities to improve support and training processes.

3.13.9 The contractor shall simulate or recreate user problems to resolve operating system difficulties.

3.13.10 The contractor shall recommend systems modifications and upgrades to reduce user problems.

3.13.11 The contractor shall maintain technical proficiency and vast technical knowledge in field of expertise.

3.13.12 The contractor shall escalate more complex problems to senior level for resolution.

3.13.13 The contractor shall provide support to end users focusing on operations, hardware, software, and network connectivity.

3.13.14 The contractor shall image, configure and install computer systems and peripherals; provide applications analysis, review, evaluation, troubleshooting, integration, security, and maintenance support for the JCSE garrison LAN/WAN.

3.13.15 The contractor shall perform duties as follows:

3.13.16 Answer requests by the trouble-ticket Help Desk, telephone, or email for IT support.

3.13.17 Assist with problem identification and resolution by assisting end users as the first and/or second level of support or by determining escalation priority to the appropriate information systems personnel.

3.13.18 Assist with maintaining technical libraries and lessons learned documentation. Coordinate the repair of computers with users and other internal staff or with outside service repair technicians.

3.13.19 Assist in the turn-in of outdated and/or inoperable automated data processing equipment (ADPE) to the Defense Reutilization and Marketing Office (DRMO).

3.13.20 Develop knowledge and technical skills on a continuous basis to stay abreast of current trends and developments in information technology.

3.13.21 Comply with all JCSE information security policies and directives.

3.13.22 Mobile device setup configuring and troubleshooting.

13.13.23 IT asset management.

13.13.24 Assist end users with audio visual requests.

13.14 Tier-2 Helpdesk Support Required Skills and Abilities:

13.4.1 Strong working knowledge of Microsoft operating systems, products, and applications, Remedy Service Desk, and hardware/software troubleshooting techniques.

13.4.2 Ability to operate and maintain large databases supporting garrison equipment inventory, blackberry allocation/billing, Remedy tracking database, and equipment parts database.

13.4.3 Comfortable working with technology and applications.

13.4.4 Good inter-personal and communications skills. Meets with key staff members to address Help Desk issues within two hours of notification.

13.4.5 Good problem diagnosis and resolution skills.

13.4.6 Excellent attention to detail and follow-up skills.

13.4.7 Ability to work as a team player and provide professional customer service.

13.4.8 The Help Desk Analyst Support contractor requires a minimum of a current IAT II certification (GSEC or Security +CE or SSCP). Contractor must meet professional certification upon appointment.

13.4.9 Must have a minimum of four (4) years' experience in IT customer support.

13.4.10 Contractor must have a Top Secret clearance.

4. DELIVERABLES

4.1. The Contractor shall maintain personnel strength IAW PWS with no lapse below 90%, with vacancies filled within two weeks.

4.2. Contractor shall provide daily personnel status report if personnel will not be present for duty and this absence is not annotated on leave report, etc., electronically, to COR NLT 0900 hours daily. The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract via a secure data collection site. The contractor is required to completely fill in all required data fields at http://www.ecmra.mil.

4.3. The Service Provider/Contractor shall provide the COR a complete, legibly typed monthly operational status report electronically, no later than the 15th monthly.

4.4. The Service Provider/Contractor shall provide the COR a complete, legibly typed monthly financial status report that will provide Status by CLIN: Planned, Received to Date, Expended, Total Expected; Travel, ODC; Summary of all CLINs; and Status by PWS element, electronically, no later than the 15th monthly.

4.5. The Service Provider/Contractor shall provide the COR a complete, legibly typed, monthly leave forecast report electronically, no later than the 15th monthly.

4.6. Quality: The contractor will complete, implement and make the Quality Control Plan available to the government for review within thirty days after contract award and all revisions to that plan will be made available to the COR.

4.7. Travel. The Contractor shall prepare and submit Trip Reports electronically to the COR within 3 days after completion of trip, meeting attendance, workshops, conferences, etc., with no more than 2 late reports.

4.8. Contractor Summary Resume(s). The Contractor shall provide customer with Contractor' Summary Resume prior to contractor reporting to work site.

4.9. SERVICES SUMMARY

#	PERFORMANCE OBJECTIVE	PWS PARAGRAPH	PERFORMANCE THRESHOLD	SURVEILLANCE METHOD
1	Provide Network Operations support tasks	Throughout PWS 3.1 – 3.10	Technically proficient managers, engineers, and administrators	DIRECT OBSERVATION
2	Contractor personnel operationally competent	3.1 – 3.10	No repeat errors in a 3 month period	DIRECT OBSERVATION
3	Provide globally deployable personnel capable of deploying within 72 hours after notification	1.6.4	Required security clearances, passports, medical and physical readiness loaded in Synchronized Pre-Deployment and Operational Tracker (SPOT). 99% error free entries with immediate corrections	AS REQUIRED

			when notified by SPOT administrator.	

5. GOVERNMENT-FURNISHED PROPERTY AND SERVICES:

5.1. Facilities: The Government will provide the necessary workspace for contractor staff to provide the support outlined in the PWS to include desk space, telephones, and other items necessary to maintain an office environment. Office spaces could also be in a tactical environment (tent, portable building, etc.….)

5.2. Office Space: The government will provide, and/or make available, administrative office space as described in this document. Government facilities comply with Occupational Safety and Health Administration (OSHA) work-place standards. Should hazards be identified, contractor will notify the government in writing, and the government will correct the hazard, taking into account safety and health priorities. Compliance with OSHA and other applicable laws and regulations for the protection of employees is exclusively the obligation of contractor. The government assumes no liability or responsibility for contractor's compliance or noncompliance with such responsibilities. Contractor shall not alter or modify the furnished office space without specific written permission from the government. Contractor shall return all facilities and equipment to the government at the end/termination of the contract. The office space and equipment provided for use in the performance of this contract shall be used only for performance of this contract. Office spaces could also be in a tactical environment (tent, portable building, etc.….).

5.3. Utilities: All utilities in the facility will be available for contractor's use in performance of tasks outlined in this PWS. Contractor shall instruct employees in utilities conservation practices. Contractor shall be responsible for operating under conditions that preclude the waste of utilities. (a) Lights must be used only in areas where work is actually being performed. (b) Employees must not adjust mechanical equipment controls for heating, ventilation, and air conditioning systems. (c) Water faucets or valves must be turned off when not in use.

5.4. Equipment: The Government will provide or make available Computers for contractor's use in performance of the tasks outlined in this PWS, as applicable. Government cell phones may be issued the contractor, which the Director(s) have identified and approved, that will require the use of the phone in performance of tasks outlined in this PWS. All materials and equipment will remain the property of the Government and will be returned upon request or at the end of the period of performance. DD Form 1149 and/or AF Form 1297 will be used for accountability and transfer between government and the contractor.

5.5. Materials: The Government will provide all materials, such as Standard Operating Procedures and Policies for contractor's use in performance of the tasks outlined in this PWS.

6. **Contractor Personnel Authorized to Accompany U.S Armed Forces Deployed Outside of the United Stated.**

   All deploying personnel must meet the minimum medical screening requirements and received all required immunizations as specified by the deploying Commander. The Government will provide, at no cost to contractor, any theater-specific immunizations and/or medications not available to the general public. The contractor should have 90 days of require medicines or have the capabilities to obtain within a 24 hour notice.

7. **Classified Information:** Disclosure of information, to any person not entitled to receive it, or failure to safeguard any classified information that may come to contractor, or any person under their control, may subject contractor, their agents or employees, to criminal liability under 18 U.S.C. §793 and §798.

8. **Breach of Security:** Neither contractor nor any of its personnel shall disclose nor cause to be disclosed any information concerning operations which could result in or increase the likelihood of the possibility of a breach of the activity's security or interrupt the continuity of operations

9. **Limitation of Government's obligation:**
   - 9.1. In event of Continuing Resolution Amendment and government' inability to fund this contract in its entirety, the government reserves the right to incrementally fund contract Line Items on a quarterly basis. For these item(s), the sum of the total price is presently available for payment and allotted to this contract. An allotment schedule is set forth in paragraph 9.10.
   - 9.2. For item(s) identified in paragraph 9.10 of this clause, the Contractor agrees to perform up to the point at which the total amount payable by the Government, including reimbursement in the event of termination of those item(s) for the Government's convenience, approximates the total amount currently allotted to the contract. The Contractor is not authorized to continue work on those item(s) beyond that point. The Government will not be obligated in any event to reimburse the Contractor in excess of the amount allotted to the contract for those item(s) regardless of anything to the contrary in the clause entitled "Termination for Convenience of the Government." As used in this clause, the total amount payable by the Government in the event of termination of applicable contract line item(s) for convenience includes costs, profit, and estimated termination settlement costs for those item(s).
   - 9.3. Notwithstanding the dates specified in the allotment schedule in paragraph 9.10 of this clause, the Contractor will notify the Contracting Officer in writing at least ninety days prior to the date when, in the Contractor's best judgment, the work will reach the point at which the total amount payable by the Government, including any cost for termination for convenience, will approximate 85 percent of the total amount then allotted to the contract for performance of the applicable item(s). The notification will state (1) the estimated date when that point will be reached and (2) an estimate of additional funding, if any, needed to continue performance of applicable line items up to the next scheduled date for allotment of funds identified in paragraph 9.10 of this

clause, or to a mutually agreed upon substitute date. The notification will also advise the Contracting Officer of the estimated amount of additional funds that will be required for the timely performance of the item(s) funded pursuant to this clause, for a subsequent period as may be specified in the allotment schedule in paragraph 9.10 of this clause or otherwise agreed to by the parties. If after such notification additional funds are not allotted by the date identified in the Contractor's notification, or by an agreed substitute date, the Contracting Officer will terminate any item(s) for which additional funds have not been allotted, pursuant to the clause of this contract entitled "Termination for Convenience of the Government."

9.4. When additional funds are allotted for continued performance of the contract line item(s) identified in paragraph 9.10 of this clause, the parties will agree as to the period of contract performance which will be covered by the funds.

9.5. If, solely by reason of failure of the Government to allot additional funds, by the dates indicated below, in amounts sufficient for timely performance of the contract line item(s) identified in paragraph 9.10 of this clause, the Contractor incurs additional costs or is delayed in the performance of the work under this contract and if additional funds are allotted, an equitable adjustment will be made in the price or prices (including appropriate target, billing, and ceiling prices where applicable) of the item(s), or in the time of delivery, or both. Failure to agree to any such equitable adjustment hereunder will be a dispute concerning a question of fact within the meaning of the clause entitled "Disputes."

9.6. The Government may at any time prior to termination allot additional funds for the performance of the contract line item(s) identified in paragraph 9.10 of this clause.

9.7. The termination provisions of this clause do not limit the rights of the Government under the clause entitled "Default." The provisions of this clause are limited to the work and allotment of funds for the contract line item(s) set forth in paragraph 9.10 of this clause. This clause no longer applies once the contract is fully funded except with regard to the rights or obligations of the parties concerning equitable adjustments negotiated under paragraph 9.10 of this clause.

9.8. Nothing in this clause affects the right of the Government to terminate this contract pursuant to the clause of this contract entitled "Termination for Convenience of the Government."

9.9. Nothing in this clause shall be construed as authorization of voluntary services whose acceptance is otherwise prohibited under 31 U.S.C. 1342.

9.10. The parties contemplate that the Government will allot funds to this contract in accordance with the following schedule:

9.10.1. On execution of contract- Base Year Total and option years

10. Invoice Requirements

An invoice for completion of each deliverable or monthly support effort for work performed the prior month shall be electronically delivered to the Client Representative via the GSA electronic contract management system by the 15th business day of each month for client acceptance. A copy of the invoice shall be attached to the associated deliverable "Acceptance Report" posted in GSA Information

Technology Solution Shop (ITSS) located on the web at https://web.itss.gsa.gov/Login. The invoice shall be submitted on official company letterhead.

For reimbursable expenses, the invoiced charges shall not exceed the limit specified in the task order. No charges will be paid by the Government, which are not specifically identified in the task and approved in advance by the Government. Copies of receipts, travel vouchers, etc., completed in accordance with Government Travel Regulations shall be attached to the invoice to support charges other than labor hours. Original receipts shall be maintained by the contractor and made available to Government auditors upon request.

10.1 Payment Information

Failure to enter an invoice into the GSA ITSS web-based system may result in a rejection. The contractor shall provide the following payment information for GSA use. It must be an exact match with the information under the contract/task order number in the GSA ITSS Contract Registration (not the contractor's company or individual representative's registration) as well as with the information under the contractor's DUNS number in the Central Contractor Registration (CCR), http://www.ccr.gov. Mismatched information may result in rejected requests for payment.

Company Name – Legal Business Name and DBA (Doing Business As)

Name

Mailing Address – Contact and Address Information

Remittance Address – Remit To Address Information

Employer's Identification Number – Federal Tax ID

DUNS (Data Universal Numbering System)

10.2 Invoice Information

The invoice shall include the labor charges and other direct costs (ODCs) authorized by the COR which are within scope of this task order (e.g., travel and/or materials) and reflect the details specified below.

- Invoice Number – must not include any special characters; ITSS and the invoice must match
- ACT Number from GSA Form 300, Block 4
- GSA Task Order Number – must match ITSS
- Contract Number from GSA Form 300, Block 3
- Point of Contact and Phone Number
- Period of Performance for the Billing Period
- Total invoiced and cumulative Labor charges by Deliverable and skill level.

- Total invoiced and cumulative Reimbursable Costs. (These must be individually itemized and specified by individual category. Categories are Travel, Training, and Material ODCs).

- Total invoiced and cumulative Travel Itemized by Individual and Trip (if applicable) Travel charges must include the traveler's name, location, and dates of travel.

- Total invoiced and cumulative Material ODCs and Support Items Itemized by Specific Item, dates delivered, and Amounts.

- Total invoiced and cumulative Indirect charges.

- Grand Total for the Invoice and Cumulative Billed to Date Amounts

- Unbilled Total

- Burn Rate

- Prompt Payment Discount, if offered

10.3 Invoice Submittal

Each invoice must be submitted at the same time to two (2) separate locations:

1) Electronically via GSA's IT Solutions System located at https:\\web.itss.gsa.gov)

2) and electronicaly to GSA's Ft. Worth Finance Office via the web at www.finance.gsa.gov or mail a hardcopy to:

GSA BCEB

PO BOX 219434, Fund 299X

KANSAS CITY, MO 64121-9434

10.3.1 The COR has to evaluate the charges detailed in the invoice submitted by the contractor and accept and certify the invoice in ITSS. The GSA CAM must validate and approve the invoice in GSA's ITSS system prior to payment of the invoice.

10.3.2 Final Invoice.

Invoices for final payment must marked with the word FINAL (even if it is a zero amount) and submitted within 60 days from task completion. The contractor shall request from GSA an extension for final invoices that may exceed the 60-day time frame.

10.3.3 The invoice information posted in ITSS must match the invoice information submitted to GSA's Finance Center to initiate a receiving report. The payment information must be a three-way match (ITSS, GSA Finance Center, and CCR) for the invoice to be successfully processed for payment.

10.3.4. Task Order Closeout

After the final invoice has been paid the Contractor shall furnish a completed and signed Release of Claims to the Contracting Officer. This release of claims is due within fifteen (15) calendar days of final payment.

10.4 Invoicing Reimbursable Costs

Reimbursable costs must not exceed the limit(s) specified in the task order. The Government will not pay charges that are not specifically identified and approved, in advance, by the Government. Copies of receipts, travel vouchers, etc. that have been completed in accordance with Government JTRs shall be attached to the invoice to support charges other than employee labor hours.

The amount invoiced shall include labor charges for actual hours worked and other direct costs (ODCs) which may be authorized by this task order (e.g., travel). For ODCs, invoiced charges shall not exceed the limit specified in the task order. No charges will be paid by the Government, which are not specifically identified in the task and approved in advance by the Government. Copies of receipts, travel vouchers, etc., completed in accordance with Government Travel Regulations shall be attached to the invoice to support charges other than personnel hours. Original receipts shall be maintained by the contractor and made available to Government auditors upon request.

10.5 Payment Schedule

The monthly charges shall be calculated by utilizing the dollar amount of the applicable period (base year or option year) divided by the number of months in that particular period in addition to authorized reimbursable costs.

11. Personal Services

GSA will not issue contracts/task orders to provide services prohibited by FAR Part 37.1. The administration and monitoring of the contractor's performance by GSA or the Client Representative shall not be as detailed or continual as to constitute supervision of contractor personnel. Government personnel may not perform any supervisory functions for contractor personnel, such as interviewing, appraising individual performance, scheduling leave or work, or directing how to perform work.

GSA meets the needs of its clients for support through non-personal services contracts/task orders. To counter the circumstances that infer personal services and to preserve the non-personal nature of the contract/task order, the contractor shall adhere to the following guidelines in the performance of the task.

a. Provide for direct supervision of all contract employees assigned to the task.

b. Refrain from discussing the issues such as skill levels and hours, salaries, cost and funding data, or administrative and personnel matters affecting contractor employees with the client.

c. Ensure close communication/coordination with the GSA Customer Account Manager, reporting problems to them as they occur (not waiting for a meeting).

d. Do not permit Government officials to interview potential contractor employees, discuss individual performance, approve leave or work scheduling of contractor employees, terminate

contractor employees, assist contractor employees in doing their jobs or obtain assistance from the contractor in doing Government jobs.

e. Do not assign contractor personnel to work under direct Government supervision.

f. Maintain a professional distance from Government employees.

g. Provide contractor employees with badges, if appropriate, identifying them as contractors.

h. Ensure proper communications with the Government. Technical discussions and Government surveillance are acceptable, but the Government cannot tell the Contractor how to do the job.

i. Assign a task leader to the order. The task leader or alternate shall be the only one who accepts tasking from the assigned Government point of contact or alternative.

12. Kick Off Meeting

Within ten (10) work days following the contract award, the contractor shall attend a “kick-off” meeting on a date to be jointly determined to review the contract terms and conditions including project transition. The meeting location will be determined after award. The meeting shall include discussion of the goals and objectives of the AF and discuss technical and administrative reporting requirements.

13. Past Performance Information

The Government will provide and record Past Performance Information for acquisitions over $150,000 utilizing the Contractor Performance Assessment Reporting System (CPARS). The CPARS process allows contractors to view and comment on the Government's evaluation of the contractor's performance before it is finalized. Once the contractor’s past performance evaluation is finalized in CPARS it will be transmitted into the Past Performance Information Retrieval System (PPIRS). Contractor’s are required to register in the CPARS, so contractor’s may review and comment on past performance reports submitted through the CPARS. The CPARS and PPIRS websites are as follows:

CPARS https://www.cpars.csd.disa.mil/

PPIRS http://www.ppirs.gov

14. The following clauses are hereby incorporated by reference:

FAR Clause	Title
52.203-3	Gratuities (Apr 1984)
52.203-19	Prohibition on Requiring Certain Internal Confidentiality Agreements or Statements (Jan 2017)

52.204-2 Security Requirements (Aug 1996)

52.204-13 System for Award Management Maintenance (Oct 2016)

52.209-9 Updates of Publicly Available Information Regarding Responsibility Matters (Jul 2013)

52.212-4 Contract Terms and Conditions – Commercial Item (Jan 2017)

52.232-39 Unenforceability of Unauthorized Obligations (Jun 2013)

52.232-40 Providing Accelerated Payments to Small Business Subcontractors (Dec 2013)

DFARS Clause Title

252.201-7000 Contracting Officer's Representative (Dec 1991)

252.203-7000 Requirements Relating to Compensation of Former DoD Officials (Sep 2011)

252.203-7001 Prohibition on Persons Convicted of Fraud or Other Defense-Contract-Related Felonies (Dec 2008)

252.203-7002 Requirement to Inform Employees of Whistleblower Rights (Sep 2013)

252.204-7000 Disclosure of Information (Oct 2016)

252.204-7003 Control of Government Personnel Work Product (Apr 1992)

252.204-7005 Oral Attestation of Security Responsibilities (Nov 2001)

252.204-7008 Compliance with Safeguarding Covered Defense Information Controls (Oct 2016)

252.204-7009 Limitations on the Use and Disclosure of Third-Party Contractor Reported Cyber Incident Information (Oct 2016)

252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting (Oct 2016)

252.204-7015 Notice of Authorized Disclosure of Information for Litigation Support (May 2016)

252.205-7000 Provision of Information to Cooperative Agreement Holders (Dec 1991)

252.209-7004 Subcontracting with Firms That are Owned or Controlled by the Government of a Terrorist Country (Oct 2015)

252.223-7004 Drug Free Work Force (Sep 1988)

252.223-7006 Prohibition on Storage, Treatment, and Disposal of Toxic or Hazardous Materials (Sep 2014)

252.227-7014 Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation (Feb 2014)

252.227-7016 Rights in Bid or Proposal Information (Jan 2011)

252.227-7019 Validation of Asserted Restrictions—Computer Software (Sept 2016)

252.227-7037 Validation of Restrictive Markings on Technical Data (Sept 2016)

252.232-7010 Levies on Contract Payments (Dec 2006)

252.237-7010 Prohibition on Interrogation of Detainees by Contractor Personnel (Jun 2013)

252.243-7002 Requests for Equitable Adjustment (Dec 2012)

Clauses By Full Text:

52.217-8 Option to Extend Services.

As prescribed in 17.208(f), insert a clause substantially the same as the following:

Option to Extend Services (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within **30** [insert the period of time within which the Contracting Officer may exercise the option].

(End of clause)

15. APPENDICES

15.1. Appendix A – MacDill AFB Contractor Security

15.2. Attachment 1 – Memorandum for 6 SFS/Visitor Reception Facility Request For Background Check/Entry Access List (EAL)

15.3. Attachment 2 – Memorandum for 6 SFS/S5B, Base Pass, Request for Issuance of AF Form 75

APPENDIX A

CONTRACTOR SECURITY

MACDILL AIR FORCE BASE, FLORIDA

INSTALLATION ENTRY CONTROL PROCEDURES FOR ALL CONTRACTORS

The following appendix provides information from Air Force Instruction 31-101 and local supplements on requirements for entering and conducting business while on MacDill Air Force Base (MAFB), Florida.

1. Contract Award.

1.1. Upon award of a contract, the contractor (including Small Purchase contractors), will have background checks conducted on all employees (including subcontractors or temporary employees) requiring access to MAFB.

1.2. The base Point of Contact (POC) is the unit or the base contracting office administratively who services the contract. The authorized format used for submitting employee personal information for background checks is located at Attachment 1, Request for Background Check.

1.3. Contractor is responsible for providing their employees' personal information to their base POC. Failure to provide all personal information required or providing fraudulent information will result in the employee's base access being denied.

1.3.1. Full name to include middle names or any known alias.

1.3.2. Date of Birth.

1.3.3. Social Security number.

1.3.4. Driver's license number and state of issue.

1.3.5. Project name and contract number.

1.3.6. Requestor's name.

1.4. Each base POC is appointed by their commander or management director on DD Form 577, Appointment/Termination Record – Authorized signature, and forwards a signed copy to the Visitor's Reception Facility (VRF) annually.

1.5. The base POC sends a request, via email, to the 6 SFS/Background Check email address, which can be located on the Global Listing (MacDill). Personal employee information will be included on Attachment 1, Request for Background Check/Entry Access List (EAL).

1.6. The 6th Security Forces Squadron (6 SFS) will, upon receiving the EAL from the base POC, conduct a background check of contractor personnel using the approved local, state, and federal government web sites.

1.7. Any contractor employee found to have a criminal conviction listed below or have an outstanding warrant(s) will not be allowed entry to the base.

1.7.1. US Citizenship, immigration status, or Social Security Account Number that cannot be verified.

1.7.2. Barred from entry/access to any military installation or facility.

1.7.3. Wanted by federal or civil law enforcement authorities, regardless of offense/violation.

1.7.4. Name appears on any federal agency's "watch list or "hit list" for criminal behavior or terrorist activity.

1.7.5. Any conviction for firearms or explosive violations within the last three years.

1.7.6. Incarcerated for 12 months or longer within the past three years, regardless of the offense.

1.7.7. Any conviction of espionage, sabotage, treason, terrorism, murder.

1.7.8. Conviction of a sexual assault, armed assault/robbery, rape, child molestation or kidnapping.

1.7.9. Drug possession with intent to sell or drug distribution.

1.8. Upon completion of the background check, the results will be electronically mailed to the requesting base POC. The email response will state whether the applicant is approved, denied, or pending further review by 6 SFS/S5 and base legal. Contract employee(s) approved for base access will report to the VRF, Building 1089 to retrieve the AF Form 75, Visitor Pass.

1.9. Background checks are valid for two years unless the person is terminated from the job, or is involved in a serious offense as listed paragraph 1.7. Requests for base access exceeding the two year period will require another background check.

1.10. The base POC identifies and appoints responsible contractor supervisor to sponsor sub-contractor and contract workers on base to perform services for no more than five business days (short-term) without a completed background check. Subsequent sponsorship (long-term) will require the proper completed background check by the VRF.

1.11. The base POC is responsible for identifying and retrieving all AF Form 75's from the contract employees once the contract has expired or the contract employee's employment is terminated and returns the passes to the VRF.

2. Contractor Visitor Passes for Entry to MAFB

2.1. The base POC completes Attachment 2, Request for Issuance of AF Form 75, and the contract employee hand carries the request to the VRF for issuance of the AF Form 75 for the duration of the contract, not to exceed one year.

2.2. Contractor must possess the proper photo identification media (driver's license/state identification card, military identification card, or other authorized U.S. governmental photo media) to be issued a base pass. Non-U.S. citizens must provide original Immigrations & Naturalization Service photo media and Social Security card.

3. Contractor Vehicle Passes for Entry to MAFB.

3.1. Operators of vehicles must provide the following documentation to register vehicles.

3.1.1. Valid driver's license.

3.1.2. Valid vehicle registration or rental agreement.

3.1.3. Valid insurance (except fleet vehicles) or rental agreement.

3.1.4. Drivers of borrowed vehicles must present a valid registration, insurance card (or policy), and power-of-attorney in the owner's name.

3.2. Operators are required to sign a consent to search and impoundment disclaimer upon receiving their vehicle pass.

4. Contract, Commercial, and/or Oversized Vehicles

4.1. All contractor, commercial, and oversized vehicles must enter MAFB through the Tanker Way Gate located off Interbay Boulevard.

4.2. The following are considered "commercial or oversized" vehicles.

4.2.1. All vehicles registered and licensed with "commercial" license plates, regardless of state of issue.

4.2.2. All vehicles, regardless of type, license plate, or size having more than two axles.

4.2.3. All vehicles displaying a commercial plaque, logo, or emblem.

5. Contractor Vehicle and Personnel Processing Requirements

5.1. The Tanker Way Gate is open for personnel and vehicle processing from 0530 – 1700 hours Monday through Friday and 0530-1000 on Saturday. Holiday hours are 0530- 1000; Thanksgiving, Christmas Eve, Christmas and New Year's Day the gate will be closed.

5.2. During closure of Tanker Way Gate, contractor/commercial vehicles requesting entry will use the Dale Mabry Gate.

6. Subcontractors

6.1. All subcontractors are required to follow the same instructions listed above for their personnel.

6.2. Contractor with an immediate access requirement for a short-term subcontractor must coordinate with their base POC prior to access authorization.

6.3. Short term subcontractor will be issued a pass not to exceed one week.

7. Contractor working in USAF Restricted Areas

7.1. Contract employees will be required to obtain a favorable National Agency Check (NAC). Contract employees will be required to complete a Standard Form 85P, a Questionnaire for Public Trust Position, before being granted access to restricted areas.

7.1.1. Contract employee/s will coordinate with the unit security manager (SM) to complete the SF 85P.

7.1.2. The SM will complete an AF Form 2583, Request for Personnel Security Action. The medical records check portion of this form is not required.

7.2. The SM will make an appointment with 6 SFS/S5I, Personnel Security office, for the contract employee to submit SF 85P.

7.3. After completion of a favorable local files check the contract employee will be eligible for the issuance of a restricted area badge on an interim basis based on submission of the SF 85P to S5I. Coordinate with the SM to complete Phase I Orientation Training as outlined in AFI 31-101, para. 7.2.2. The SM will provide the contract employee with AF Form 2586, Unescorted Entry Authorization Certificate, with instructions on completing the form.

7.4. Contractor will return to 6 SFS/S5R, Bldg. 528, to obtain an Air Force Entry Control Card (AFECC).

7.5. Issues identified during the course of the investigation may result in immediate revocation of restricted area access.

7.6. Any work on or near the flight line will be coordinated through the MacDill Flight line Constable located in bldg. 528. The Flight line Constable will verify the need to access the restricted area and determine if a Free Zone can be established.

7.7. Access to Tenant Units.

7.7.1. The contractor requiring unescorted access to USCENTCOM, USSOCOM, MARCENT, and SOCCENT facilities, a favorable NAC is required for entry to the facilities. For access into these facilities, the contractor will contact JCSE Personnel Security office at (813) 828-6073 for the issuance of the appropriate USCENTCOM access.

8. Flight line Driving.

8.1. Only authorized contracted or privately owned vehicles with colored cones are authorized on the flight line. Base operations will issue colored cones. The cone must be visible at all times when operating a vehicle on the flight line. The cone must be secured when not in use.

8.2. Contractor will never enter restricted areas unless properly escorted or authorized by the installation commander or designee through the issuance of an AFECC.

8.3. If security forces or a military member detains a contractor or contract employee at any time or for any reason, contractor will comply with their request and will not become combative or argumentative.

9. Miscellaneous Requirements

9.1. All requests for additional contract employees must meet the same requirements listed in paragraph 1, before vehicle passes will be issued.

9.2. The 6th Contracting Office will be notified when personnel leave contractor company for any reason. The 6th Contracting Officer will provide that information to the VRF to ensure the EAL is updated.

9.3. Contractor is responsible for the return of all identification media and vehicle passes at the end of the contract or when personnel depart for any reason. All identification media and passes issued by security forces will be returned to the VRF. CAC cards issued will be returned to the Trusted Agent (TA). Failure to comply with these requirements may result in withholding of final payment.

9.4. During increased Force Protection Conditions (FPCONs) there may be limited entry to the installation.

9.5. Contractor ARE NOT AUTHORIZED to escort (vouch) any personnel entering MAFB unless designated by base POC.

9.5.1. Exceptions to this rule will be addressed on an as needed basis through the Contracting Officer.

9.5.2. The escorting contractor will be responsible for all individuals they escort onto the installation. Contractor with installation access vouching authority will be authorized to vouch for personnel not to exceed one week.

9.5.3. Contractor escort privileges will be revoked if its determined contractor is attempting to supersede normal installation access requirements.

9.6. Any contractor found in violation of this requirement will be escorted off the installation. They will be removed from the company EAL and not be allowed to reenter MAFB without the written permission of the installation commander.

9.7. Contractor is required to obey all entry requirements, traffic rules and regulations IAW AFI 31-204, MACD SUP 1, Traffic Supervision. Failure to comply with requirements could result in disbarment from the installation.

9.8. Where applicable, contractor must establish and maintain a Visitor/Vehicle Pass tracking system. This list shall be provided to the Contracting Officer prior to the contract start date and made available during contract performance on request.

10. Badges and Identification Media

10.1. Common Access Cards (CAC) will be issued in accordance with Air Force Federal Acquisition Regulation Supplement (AFFARS) Subpart 5352.242-9001, CACs for Contractor Personnel to all contract employees requiring network computer access. All contractor employees requesting a CAC will be required to obtain a favorable National Agency Check (NAC). Follow guidance in paragraph 7.1 and 7.2 above when submitting an employee for a NAC. Contractor personnel request for CACs will be submitted through the organization TA utilizing contractor Verification System (CVS). The TA will initiate and approve the request in CVS. Once the request is approved, contractor will report to the Military Personnel Flight, 6th Mission Support Squadron, Bldg. 373 to receive a CAC.

11. Contact Information.

11.1. Questions regarding base access will be directed to VRF, (813) 828-2737 or (813) 828-3809.

11.2. Security related matters should be directed to the Security Forces Control Center, (813)828-3322-/3323/3324.

12. Attachment 1 – [YOUR COMPANY LETTERHEAD]

DATE:

FROM: (Your Company Address Information)

MEMORANDUM FOR 6 SFS/VISITOR RECEPTION FACILTIY

SUBJECT: Request For Background Check/Entry Access List (EAL)

1. The (Your Company Name) will be working on Contract Number (Example: F12958- 06-C-0092) for the purpose of building the new Temporary Lodging Facility near bldg. 2717 from 1 May 2006 through 31 May 2008.

2. My onsite POC will be first & last name, and his on-site phone number is (xxx) xxx- xxxx.

3. The MacDill AFB Unit POC is first & last name from the (insert unit name example: 6 SFS, 819 GRS, (6 CES), his phone number (xxx) xxx-xxxx.

4. The Procurement/Administrative Contracting Officer is first & last name and her phone number is (xxx) xxx-xxxx.

5. The following personnel will be required to access MacDill AFB on a daily basis for the length of the contract.

LAST NAME	FIRST NAME	M.I.	DOB	SSN	DRIVERS LICENSE #	ISSUING STATE
DOE	JOHN	NMI	07/17/78			FL

6. If there are any questions, please contact me at (xxx) xxx-xxxx.

Signature Block of Company

Approving Official

13. Attachment 2 – (OFFICIAL UNIT LETTERHEAD)

DATE:

MEMORANDUM FOR 6 SFS/S5B

(Pass Request not valid 10 days from date stamp)

FROM:

SUBJECT: Request for Issuance of AF Form 75

1. Request an AF Form 75 be issued to the person indicated below:

NAME:

(Last, First, Middle Initial)

SSN: Date Of Birth (Day/Mon/Yr.): _____

FDL: INS# _____

SPONSOR'S NAME:

CONTRACT NO.:

EXPIRATION OF CONTRACT/AUTHORIZATION:

LOCATION OF EMPLOYMENT ON BASE:

HOURS/DAYS AUTHORIZED ON BASE:

2. I certify the above individual is on base for employment as noted and approve the request for issuance of a base pass for the period indicated above. This vehicle pass is issued with the understanding that the individual identified herein will be the exclusive driver of this vehicle.

Certifying Official Full Name (Printed)/Title/Phone Signature

---

TO: 6 SFS Visitor's Reception Facility

I have provided true and accurate information in order to obtain a temporary pass. I also understand my pass can be confiscated by Sponsor or MacDill AFB Security Forces at any time.

Employee Signature Date

Information protected by the "Privacy Act of 1974"

IMPORTANT: The possession and use of the AF form 75 is intended solely for the individual listed above during performance of contractual duties. Any other use or transfer of the pass is strictly prohibited.